State of Iowa Enterprise Interconnectivity Standard

June 8, 2007

Purpose

This document provides minimum requirements to establish, maintain, and terminate interconnections between information technology (IT) systems owned, operated or managed by: State of Iowa agencies; the Information Technology Enterprise (ITE); and the Iowa Communications Network (ICN).

Overview

The State of Iowa maintains a variety of data in its IT systems, including confidential and sensitive customer information. Agencies connecting to IT systems outside of their agency face a higher risk to the confidentiality, integrity and availability of their data. Protection of data in state systems will be enhanced by ensuring that agencies follow standards when connecting to the shared state IT infrastructure and IT systems outside state government.

Scope

For the purpose of this standard, security is defined as the ability to protect the confidentiality, integrity, and availability of information processed, stored and transmitted by agencies. Information technology assets covered by this policy include those that process, store, transmit or monitor digital information. This document presents minimum standards which must be met by agencies wishing to connect to the shared State IT infrastructure

If the requirements of this standard are met by another agency or a third party service provider, the service provider must sign an agreement that they will adhere to all of the requirements of this standard.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Connectivity Standard are defined below:

- **Access Control:** The process of granting access to information technology (IT) system resources only to authorized users, programs, processes, or other systems.

- **Access Control List (ACL):** A register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.

- **Authentication:** The process of verifying the authorization of a user, process, or device, as a prerequisite for granting access to resources in an IT system.

- **Disconnection:** The termination of an interconnection between two or more IT systems. A disconnection may be planned (e.g., due to changed business needs) or unplanned (i.e., due to an attack or other contingency).

- **Encryption:** The translation of data into a form that is unintelligible without a deciphering mechanism.

- **Firewall:** A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

- **Iowa Communications Network (ICN):** The Iowa Communications Network is a state agency that administers a statewide fiber optics network.

- **Identification:** The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

- **Interconnection or interconnectivity:** The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

- **Information Technology Enterprise (ITE):** An enterprise within the Iowa Department of Administrative Services. ITE's primary responsibilities are in the areas of providing information technology, developing and implementing recommended standards for information technology, developing and maintaining security policies and systems and coordinating the acquisition of information technology by participating agencies.

- **Least Privilege:** The security objective of granting users only those accesses they need to perform their official duties.

- **Risk:** The net mission impact considering the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur.

- **Security Controls:** Protective measures used to meet the security requirements specified for IT resources.

- **Security Incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Security Incidents pose a threat to the shared State IT infrastructure with respect to confidentiality, integrity, or availability. Examples include unintentional release of confidential data, system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, and execution of malicious code that destroys data.

- **Server:** A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

- **Virus:** A computer program containing a malicious segment that attaches itself to an application program or other executable component.

- **Virtual Private Network (VPN):** A private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks (WANs) that span large geographic areas, to provide site-to-site connections to branch offices and to allow mobile users to dial up their company LANs.

- **Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

- **Worm:** A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Updates

This standard will be reviewed at least every two years and updated as needed.

ELEMENTS OF THE STANDARD

The following enterprise connectivity elements apply to all agencies wishing to connect to the shared State IT infrastructure.

1. Auditing: All agencies shall maintain and analyze audit logs to detect and track unusual or suspicious activities.

- Develop a log review policy. Include:
  - Length of time for log retention consistent with agency activities and regulations.
  - Individual(s) responsible for log review.
  - Log review procedures including frequency of review.
- Develop baseline behavior for normal activity.

2. Communication: All agencies shall maintain communication with the Information Security Office and exchange information regularly with the Chief Information Security Officer who will in turn relay information to other agencies.

Information to be shared includes:

- Changes in management and technical personnel.
- Activities establishing, maintaining, or terminating interconnections.
- Security incidents affecting the connected systems and data.
- Disasters and other contingencies disrupting any of the connected systems.
- Planned restoration of any interconnection.

3. Emergency Disconnection: All agencies are subject to emergency disconnection from the shared State IT infrastructure.

Agencies may be disconnected after consultation with appropriate staff if:

- Their system is exploited by a virus/worm and no patch is available.
- Their system is an originator of a virus/worm and there is a high risk of infecting other systems.
- The agency is unable to resolve the issue.

Prior to disconnection agencies shall be:

- Given the opportunity to isolate and investigate the incident.
- Notified by telephone or other verbal method, and receive e-mail confirmation of the notification.
- Provided details on when and under what conditions the interconnection shall be restored.
- Except if an agency cannot be reached and an emergency exists.

4. Encryption: Agencies connecting remotely must use encryption for connection, as well as for all remote administration tasks and file transfers.

Encryption is required for:

- Virtual Private Network (VPN) connections.
- Remote administration and file transfers.

5. Firewalls: All agencies shall install firewalls at all interconnections between their agency and other agencies, third party organizations and the Internet.

- Default passwords for all firewalls must be changed before installation.
- Firewall software and/or integrated operating systems of hardware firewalls must be up to date.
- Firewalls must be configured to deny by default all incoming and outgoing transmissions.
- Only required ports shall be opened.
- Critical systems should be segregated from other systems where possible. For example use of a DMZ for web servers.
- Firewall software updates must be tested before going into production.
- Default SNMP community strings should be changed from default for all SNMP manageable devices.

6. Identification and Authentication: Agencies shall identify and authenticate users to ensure that they are authorized to access the interconnection at a minimum implementing a strong password and user ID mechanism.

Mechanisms include:

- User identification and passwords.
    - Passwords are at least eight characters.
    - Passwords are a mixture of alphabetic and numeric characters.
    - Passwords are changed at intervals of sixty days or less.
    - Master password files are encrypted and protected from unauthorized access.
- Digital certificates.
- Authentication tokens.
- Biometrics.
- Smart cards.

The mechanisms may be used by themselves or as part of multi-factor authentication.

7. Logical Access Controls: Agencies shall use Access Control Lists (ACL) and access rules to specify the access privileges of authorized personnel (or agencies if they are using a site-to-site VPN) including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search).

- ACL's should be:
    - Configured offline.
    - Versioned in a repository.
    - Distributed to the appropriate control device.
- Agencies shall grant appropriate access privileges:
    - Based on roles or job functions.
    - Based on the principle of least privilege.
- Only system administrators have access to the controls.
- A log-on warning banner approved by the agency's legal counsel shall notify users that:
    - They have accessed a State of Iowa computer system.
    - Consent to monitoring.

8. Operational Testing: Agencies shall test the interface between applications across all interconnections.

To the extent possible, agencies will test interfaces prior to establishing interconnections.

- Test security controls under realistic conditions.
- Testing shall be conducted in an isolated, non-operational environment if possible.
- Tests and the results should be documented.

9. Patch Management: All agencies must patch their systems in a timely manner.

All agencies shall establish a patch methodology.

- Patches shall be tested prior to being applied.
- Patches deemed critical by the Information Security Office (ISO) applied within five (5) work days of release by the vendor.
- ISO will notify agencies of critical patches via the Security Alert listserv or other means if email is unavailable.
- Non-critical patches shall be applied per a schedule established by the agency.

10. Physical Security: Agencies shall provide appropriate physical security for their information technology systems to prevent unauthorized access.

11. Reporting and Responding to Security Incidents: All agencies shall notify the Information Security Office of intrusions, attacks, or internal security breaches, so that other agencies can take steps to determine whether their systems have been compromised.

- The Information Security Office shall establish a reporting mechanism for agencies.

- The Information Security Office will notify agencies of incidents.
- Agencies shall take appropriate steps to isolate and respond to incidents originating from their systems.
- When appropriate, law enforcement authorities shall be notified, and all attempts should be made to preserve evidence.

12. Security Awareness and Training: Agencies shall conduct security awareness activities and training for all personnel involved in managing, using, and/or operating the interconnection.

- Provide training for new users and refresher training for all users on an annual basis.
- Establish an acceptable use policy and distribute it to all users.
- Require all users to acknowledge acceptable use rules.

13. Security Reviews: Each agency shall review their security controls at least annually, or whenever a significant change occurs, to ensure they are operating properly and are providing appropriate levels of protection.

- Annual vulnerability assessment.
- Security problems shall be documented and corrected in a timely manner.

14. Virus Scanning: Agencies shall install anti-virus software to protect all servers and computer workstations linked to the interconnection.

- Data passing between systems is scanned.
- Anti-virus software automatically checks for updates at least daily.
- Administrators are automatically notified if a detected virus cannot be cleaned.
- Users are instructed on how to report a suspected virus.
- Develop procedures and assign responsibilities for response and recovery.

Effective Date

Agencies must be fully compliant with this standard on or before October 31, 2007.

Enforcement

This standard will be enforced pursuant to Iowa Administrative Code 11—25.11(8A).